UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,487	08/16/2001	Edward W. Kohler JR.	RIV-0430	3664

87555 7590 06/04/2009

Riverbed Technology Inc. - PVF
c/o Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618

EXAMINER	
ISMAIL, SHAWKI SAIF	

ART UNIT	PAPER NUMBER
2455	

MAIL DATE	DELIVERY MODE
06/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/931,487	KOHLER ET AL.	
	Examiner	Art Unit	
	SHAWKI S. ISMAIL	2455	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date. _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

RESPONSE TO AMENDMENT

1. Claims 1, 3, 4, 6, 8-12, 15-20, 22-23 and 25-31 of this application have been amended by the applicant in response to the Board Decision rendered September 4, 2008. Claims 1-33 are pending. In view of the Decision on Appeal and subsequent search, prosecution has been reopened.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim11 recites the limitation "the control center" at line 2 of the claim.

Claim12 recites the limitation "the destination address" at line 4 of the claim.

Claim15 recites the limitation "the victim destination address" at line 10 of the claim.

Claim15 recites the limitation "the data center" at line 11 of the claim.

Claim16 recites the limitation "the control center" at line 2 of the claim.

Claim16 recites the limitation "the data center" at line 3 of the claim.

Claim17 recites the limitation "the control center" at line 2 of the claim.

Claim18 recites the limitation "the victim destination address" at line 3 of the claim.

Claim19 recites the limitation "the destination address" at line 4 of the claim.

There is insufficient antecedent basis for these limitations in the claims.

These are representative examples. Applicants should review all pending claims for similar problems. Other dependent claims, which are not specifically cited above are also rejected because of the deviancies of its respective parent claim.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-12 and 15-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yavatkar et al.,** (Yavatkar) U.S. Patent No. **6,735,702** in view of **Wetherall et al.,** (Wetherall) U.S. Patent No. **7,058,015.**

5. As to claim 1, Yavatkar teaches a method of protecting a data center against a denial of service attack, the method comprises:

sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors (refer to col. 3 line 65 – col. 4, line 23). Yavatkar discloses providing the bloodhound agents with directions (commands) to collect data throughout the network. The bloodhound agents of Yavatkar are data collectors to be deployed throughout the network and the bloodhound agents provide responses (reports) to the commands from by the watchdog agents. Yavatkar discloses launching the bloodhound agents with the directions/commands to the various points in the network and then receiving the reports based on the bloodhounds' findings (col. 3, lines 25-28, col. 4, lines 2-21, and col. 17, lines 36-37). However, Yavatkar's watchdog agents do not send queries to the bloodhound agents deployed at the different points in the network.

Wetherall teaches as illustrated in details in FIG. 2, distributively disposed sensors 104a 104c (data collectors) monitor and report on network traffic routed through routing devices 106a 106c, block 202 and back to the directors. The reporting may be self-initiated or provided in response to a request. In one embodiment, the reported data include various statistics describing the network traffic that is forwarded (col. 4, lines 40-47).

It would have been obvious to one of ordinary skill in the art to incorporate the teaching of Wetherall into the system of Yavatkar in order to allow for greater flexibility in choosing how the reporting was going to take place. This would enable the reporting in Yavatkar by the bloodhound agents (data collectors) to be self-initiated or in response to a request (query) as taught in Wetherall col. 4, lines 40-47.

sending the statistical information from the data collectors in response to the queries (col. 3 line 65 – col. 4, line 23);

processing the statistical information to determine the source of suspicious network traffic heir sent to the data center (col. 3, lines 25-37 and col. 18, lines 32-53, agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node).

6. As to claim 2, Yavatkar teaches the method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for the statistical information based on destination address for the data center (col. 13, lines 44-53 and col. 3, line 65 – col. 4, line 23, the

bloodhound agents are deployed to specific areas of the network depending on the source of the attack).

However, Yavatkar's watchdog agents do not send queries to the bloodhound agents deployed at the different points in the network.

Wetherall teaches as illustrated in details in FIG. 2, distributively disposed sensors 104a 104c (data collectors) monitor and report on network traffic routed through routing devices 106a 106c, block 202 and back to the directors. The reporting may be self-initiated or provided in response to a request. In one embodiment, the reported data include various statistics describing the network traffic that is forwarded (col. 4, lines 40-47).

It would have been obvious to one of ordinary skill in the art to incorporate the teaching of Wetherall into the system of Yavatkar in order to allow for greater flexibility in choosing how the reporting was going to take place. This would enable the reporting in Yavatkar by the bloodhound agents (data collectors) to be self-initiated or in response to a request (query) as taught in Wetherall col. 4, lines 40-47.

7. As to claim 3, Yavatkar teaches the method of claim 1 wherein processing further comprises:

Determining, from at least in part, the collected statistical information, what data centers are involved in the attack on the data center (col. 8, lines 32-53, the agents determine the source of the attack and other nodes that it affected).

8. As to claim 4, Yavatkar teaches the method of claim 3 wherein determining is performed by a control center that receives the statistical information from the data collectors, and determining further comprises:

sending data to/from a gateway device that is associated with the data center (col. 13 line 54 – col. 14, line 17, the gateway associated with the attack is identified and measures are taken to filter the attack).

9. As to claim 5, Yavatkar teaches the method of claim 4 wherein the gateway identifies the network address of the data center, via a message to the control center (col. 13 line 54 – col. 14, line 17).

10. As to claim 6, Yavatkar teaches the method of claim 5 wherein the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control enter in response to the queries sent from the central control center (see Yavatkar Fig. 3).

However, Yavatkar's watchdog agents do not send queries to the bloodhound agents deployed at the different points in the network.

Wetherall teaches as illustrated in details in FIG. 2, distributively disposed sensors 104a 104c (data collectors) monitor and report on network traffic routed through routing devices 106a 106c, block 202 and back to the directors. The reporting may be self-initiated or provided in response to a request. In one embodiment, the reported data include various statistics describing the network traffic that is forwarded (col. 4, lines 40-47).

It would have been obvious to one of ordinary skill in the art to incorporate the teaching of Wetherall into the system of Yavatkar in order to allow for greater flexibility in choosing how the reporting was going to take place. This would enable the reporting in Yavatkar by the bloodhound agents (data collectors) to be self-initiated or in response to a request (query) as taught in Wetherall col. 4, lines 40-47.

11. As to claim 7, Yavatkar teaches the method of claim 5 wherein message indicates the type of attack (col. 3, lines 35-45 and col. 4, lines 41-61).

12. As to claim 8, Yavatkar teaches the method of claim 1 wherein a source of the attack is behind a gateway (col. 13 line 54 – col. 14, line 17)

13. As to claim 9, Yavatkar teaches the method of claim 8 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway that the attacking system is behind to prevent the attacking traffic from attacking system from reaching the network (col. 13 line 54 – col. 14, line 17).

14. As to claim 10, Yavatkar teaches the method of claim 8 wherein if a source of the attack is behind a gateway, the gateway that the attacking system is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address of the data center (col. 13 line 54 – col. 14, line 17).

15. As to claim 11, Yavatkar teaches the method of claim 1 wherein if source of the attack is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attacking system (col. 13 line 54 – col. 14, line 17).

16. As to claim 12, Yavatkar teaches the method of claim 1 wherein if source of the attack is not behind a gateway, the method further comprises:

contacting administrators at locations involved in the attack to have the administrators take action to filter out packets with the destination address (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6).

17. As to claim 15, Yavatkar teaches a method of protecting a victim data center against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses (col. 13, lines 44-53);

receiving, from a gateway disposed near the victim data center, a notification that the victim data center is under an attack (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6);

sending queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network packets and collect statistical information on network packets sent over the network the queries being request for statistical information from data collectors that have examined network traffic with the victim destination address (see Yavatkar col. 3, lines 25-37 and col. 18, lines 32-53). Yavatkar discloses providing the bloodhound agents with directions (commands) to collect data throughout the network. The bloodhound agents of Yavatkar are data collectors to be deployed throughout the network and the bloodhound agents provide responses (reports) to the commands from by the watchdog agents. Yavatkar discloses launching the bloodhound agents with the directions/commands to the various points in the network and then receiving the reports based on the bloodhounds' findings (col. 3, lines 25-28, col. 4, lines 2-21, and col. 17, lines 36-37). However, Yavatkar's watchdog agents do not send queries to the bloodhound agents deployed at the different points in the network.

Wetherall teaches as illustrated in details in FIG. 2, distributively disposed sensors 104a 104c (data collectors) monitor and report on network traffic routed through routing devices 106a 106c, block 202 and back to the directors. The reporting may be self-initiated or provided in response to a request. In one embodiment, the reported data include various statistics describing the network traffic that is forwarded (col. 4, lines 40-47).

It would have been obvious to one of ordinary skill in the art to incorporate the teaching of Wetherall into the system of Yavatkar in order to allow for greater flexibility in choosing how the reporting was going to take place. This would enable the reporting in Yavatkar by the bloodhound agents (data collectors) to be self-initiated or in response to a request (query) as taught in Wetherall col. 4, lines 40-47.

determining the data center or centers involved in the attack on the victim data center by analyzing collected statistical information from the data collectors (col. 18, lines 32-53).

18. As to claim 16, Yavatkar teaches the method of claim 15 further comprising:

Communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center (col. 13 line 54 – col. 14, line 17).

19. As to claim 17, Yavatkar teaches the method of claim 16 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway to block the attacking traffic (col. 13 line 54 – col. 14, line 17).

20. As to claim 18, Yavatkar teaches the method of claim 17 wherein if a source of the attack is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 13 line 54 – col. 14, line 17).

21. As to claim 19, Yavatkar teaches the method of claim 15 wherein if a source of the attack is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6).

22. As to claim 20, Yavatkar teaches a system to thwart denial of service attacks on a victim data center, the system comprising:

a plurality of data collectors dispersed throughout a network, the data collectors collecting statistical data on network traffic (col. 3, lines 25-37 and col. 18, lines 32-53);

a control center coupled to the plurality of data collectors (refer to Fig. 1, col. 5, lines 47-67), the control center, comprising a memory; a processor; and a computer readable medium storing a computer program product the computer readable medium, comprising instructions for causing the control center to:

receive from the data center a notification that the data center is under an attack (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6); and in response to receiving the notification,

send queries to data collectors to request the statistical information collected by the data collectors based in network traffic, the statistical information used to determine the source of suspicious network traffic being sent to the data center (col. 3, lines 25-37 and col. 18, lines 32-53); Yavatkar discloses providing the bloodhound agents with directions (commands) to collect data throughout the network. The bloodhound agents of Yavatkar are data collectors to be deployed throughout the network and the bloodhound agents provide responses (reports) to the commands from by the watchdog agents. Yavatkar discloses launching the bloodhound agents with the directions/commands to the various points in the network and then receiving the reports based on the bloodhounds' findings (col. 3, lines 25-28, col. 4, lines 2-21, and col. 17, lines 36-37). However, Yavatkar's watchdog agents do not send queries to the bloodhound agents deployed at the different points in the network.

Wetherall teaches as illustrated in details in FIG. 2, distributively disposed sensors 104a 104c (data collectors) monitor and report on network traffic routed through routing devices 106a

106c, block 202 and back to the directors. The reporting may be self-initiated or provided in response to a request. In one embodiment, the reported data include various statistics describing the network traffic that is forwarded (col. 4, lines 40-47).

It would have been obvious to one of ordinary skill in the art to incorporate the teaching of Wetherall into the system of Yavatkar in order to allow for greater flexibility in choosing how the reporting was going to take place. This would enable the reporting in Yavatkar by the bloodhound agents (data collectors) to be self-initiated or in response to a request (query) as taught in Wetherall col. 4, lines 40-47.

a gateway device that passes network packets between the network and the data center, the gateway disposed to protect the victim data center, and being coupled to the control center (col. 13 line 54 – col. 14, line 17).

23. Claims 21-33 do not teach or define any new limitation beyond claims 1-20 above, therefore, they are rejected for similar reasons.

24. Claim 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yavatkar et al.,** (Yavatkar) U.S. Patent No. **6,735,702** in view of **Wetherall et al.,** (Wetherall) U.S. Patent No. **7,058,015** and further in view of **Hill et al.,** (Hill) U.S. Patent No. **6,088,804.**

25. As to claim 13 and 14, Yavatkar teaches a method for blocking denial of service and address spoofing attacks on a network (col. 13. lines 23-43). However, Yavatkar does not explicitly teach wherein the attacks are classified into categories based on the severity that they cause to the network.

Hill teaches a system and method for adaptively responding to computer network security attacks. Hill further teaches classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2; lines 53-60; col. 6, lines 9-22).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate Hill's classification of the severity of attacks into the invention of Yavatkar in order minimize the load on the computer network. Displaying attack information would help the network manager prioritize the severity of the attacks so that it spend less time countering lesser threats and more time countering severe threats (col. 2, lines 47-53).

Response to Arguments

26. Applicant's arguments have been fully considered however they deemed moot in view of the new ground(s) of rejection.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shawki S Ismail whose telephone number is 571-272-3985. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached at 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Shawki S Ismail/
Examiner, Art Unit 2455
March 25, 2009

/saleh najjar/

Supervisory Patent Examiner, Art Unit 2455

/Jack Harvey/

Director, Technology Center 2400